

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

EFREN RAMOS,
Plaintiff,
v.
THE GAP, INC.,
Defendant.

Case No. [23-cv-04715-HSG](#)

**ORDER GRANTING MOTION TO
DISMISS**

Re: Dkt. No. 16

Pending before the Court is Defendant The Gap Inc.’s motion to dismiss. Dkt. No. 16. The Court finds this matter appropriate for disposition without oral argument and the matter is deemed submitted. *See* Civil L.R. 7-1(b). For the reasons detailed below, the Court **GRANTS** the motion.

I. BACKGROUND

Plaintiff Efren Ramos filed this putative class action against Defendant The Gap, Inc. for allegedly invading customers’ privacy through the use of marketing emails and tracking software. *See generally* Dkt. No. 1 (“Compl.”). Defendant is a clothing retailer, which as relevant to this lawsuit, operates an email domain and website.¹ Defendant sends its customers periodic marketing emails, which direct them to Defendant’s website. *See id.* at ¶¶ 5, 16. According to the complaint, Defendant contracts with a third party, Bluecore, Inc., to provide software that runs on the emails to help Defendant optimize its marketing campaigns. *See id.* at ¶¶ 1–2, 9–14. The complaint alleges that Bluecore’s software embeds unique and trackable URL links into the words and images in Defendant’s marketing emails so that Defendant can assess customers’ email

¹ The email domain is bananarepublicfactory@email.bananarepublicfactory.com and the website is at <https://bananarepublicfactory.gapfactory.com>.

behavior. *See id.* at ¶¶ 2, 10–14. When a customer clicks on one of these links, Bluecore is able to capture customer data, such as the “the email address of the subscriber as well as his or her device type, geolocation, IP address and the part of the email he or she clicked on,” before directing them to the retail website. *See id.* Once on Defendant’s website, Bluecore further uses JavaScript and cookies to monitor customers’ behavior there too. *See id.* at ¶¶ 13–14. With all this information Bluecore can create a personal profile for each customer and Defendant can in turn send personalized emails to them, such as an email when a customer places a product in a cart but does not purchase the item. *See id.* The complaint alleges that Defendant and Bluecore tracked consumers in this way without their consent. *See id.* at ¶ 39.

Based on these allegations Plaintiff brings causes of action against Defendant for (1) violations of the California Invasion of Privacy Act (“CIPA”), Cal Penal Code §§ 631(a) and 635; (2) statutory larceny, Cal. Penal Code §§ 486 and 496; and (3) violations of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200, *et seq.* Defendant has moved to dismiss the complaint in its entirety. Dkt. No. 16.

II. LEGAL STANDARD

Federal Rule of Civil Procedure 8(a) requires that a complaint contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). A defendant may move to dismiss a complaint for failing to state a claim upon which relief can be granted under Rule 12(b)(6). “Dismissal under Rule 12(b)(6) is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory.” *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). To survive a Rule 12(b)(6) motion, a plaintiff need only plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when a plaintiff pleads “factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

Rule 9(b) imposes a heightened pleading standard where fraud is an essential element of a claim. *See* Fed. R. Civ. P. 9(b) (“In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake.”); *see also Vess v. Ciba-Geigy Corp. USA*, 317

1 F.3d 1097, 1107 (9th Cir. 2003). A plaintiff must identify “the who, what, when, where, and how”
 2 of the alleged conduct, so as to provide defendants with sufficient information to defend against
 3 the charge. *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997). However, “[m]alice, intent,
 4 knowledge, and other conditions of a person's mind may be alleged generally.” Fed. R. Civ. P.
 5 Rule 9(b).

6 In reviewing the plausibility of a complaint, courts “accept factual allegations in the
 7 complaint as true and construe the pleadings in the light most favorable to the nonmoving party.”
 8 *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). Nevertheless,
 9 courts do not “accept as true allegations that are merely conclusory, unwarranted deductions of
 10 fact, or unreasonable inferences.” *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir.
 11 2008) (quoting *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001)).

12 **III. DISCUSSION**

13 **A. CIPA § 631(a)**

14 Plaintiff alleges that Defendant’s conduct constitutes an illegal wiretap under CIPA
 15 § 631(a). *See* Compl. at ¶¶ 30–40. Section 631(a) contains four distinct clauses, imposing
 16 liability on “any person” who:

- 17 (i) “by means of any machine, instrument, or contrivance, or in any other manner,
 18 intentionally taps . . . any telegraph or telephone wire, line, cable, or instrument”;
- 19 (ii) “willfully reads, or attempts to read, or to learn the contents or meaning of any
 20 message, report, or communication while the same is in transit”;
- 21 (iii) “uses, or attempts to use, in any manner, or for any purpose, or to communicate in
 22 any way, any information so obtained”; and
- 23 (iv) “aids, agrees with, employs, or conspires with any person or persons to unlawfully
 24 do, or permit, or cause to be done any of the acts or things mentioned above.”

25
 26 Cal. Penal Code § 631(a); *see also Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (Cal. 1978) (en
 27 banc) (clarifying that § 631(a) imposes liability for “distinct and mutually independent patterns of
 28 conduct: intentional wiretapping, willfully attempting to learn the contents or meaning of a

communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities.”). Plaintiff appears to contend that Defendant is liable under all four clauses. *See* Compl. at ¶¶ 41–46; Dkt. No. 20 at 4–6.

In response to Plaintiff’s cause of action under § 631(a) Defendant contends that (1) it is exempt from direct liability under the CIPA as a party to the communications; (2) the first clause of § 631(a) does not apply to internet wiretaps; and (3) Plaintiff has not pled that Bluecore intercepted the protected “contents” of challenged communications. *See* Dkt. No. 16 at 5–9.

i. Direct Liability

As an initial matter, Defendant urges that it cannot be held directly liable under § 631(a) because it was a party to the challenged communications at issue here. *See* Dkt. No. 16 at 6. Plaintiff acknowledges that a party to the communication is not liable under § 631(a). *See* Dkt. No. 20 at 5; *see also In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (citing *Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (Cal. Ct. App. 1979)). Nevertheless, Plaintiff urges that Defendant was not necessarily a party to all the communications challenged in the complaint. *See* Dkt. No. 20 at 5–6.

Plaintiff suggests that Bluecore’s tracking software allows Defendant to track consumers outside the context of Defendant’s marketing emails and website. *See id.* at 6. Plaintiff points to a single sentence in the complaint, which asserts: “Bluecore’s tracking software and contractual arrangements also permitted Defendant to track its known, and unknown, userbase after they logged off the Website while those users browsed their emails.” Compl. at ¶ 37. The complaint also obliquely references collecting information about “email open rates.” *See id.* at ¶¶ 11, 19. Relying on these allegations, Plaintiff appears to suggest that Bluecore’s software allows Defendant to view information about *third-party* emails in Plaintiff’s inbox, and not just those from Defendant. *See* Dkt. No. 20 at 5–6. If Plaintiff could sufficiently allege this, it might plausibly give rise to liability under § 631(a). But that is not alleged in the operative complaint.

The complaint specifically defines emails as those “electronic communications between Defendant and its clients via emails sent from Defendant’s email domain.” *See* Compl. at ¶ 1. And the description of Bluecore’s tracking software is that it helps companies optimize their email

1 campaigns by providing them “with a detailed view of how customers are engaging with [their]
2 email templates . . . to improve email performance going forward.” *See id.* at ¶¶ 9–10. The only
3 plausible reading of the complaint as drafted is that “email open rates” refers to the rate at which
4 consumers open emails from *Defendant*. In short, there are no allegations to support Plaintiff’s
5 suggestion that Defendant somehow monitors the content of or Plaintiff’s engagement with emails
6 in Plaintiff’s inbox other than those sent by Defendant.

7 Therefore, the Court **GRANTS** the motion to dismiss to the extent Plaintiff attempts to
8 hold Defendant directly liable under § 631(a). Because Plaintiff has also alleged that Defendant is
9 liable as an “aider and abettor” under clause four, *see* Dkt. No. 20 at 4, the Court addresses
10 Defendant’s remaining arguments as to § 631(a).

11 **ii. Communications over the Internet: Clause One**

12 The first clause of § 631(a) provides that it is punishable by fine or imprisonment for “any
13 person who by means of any machine, instrument, or contrivance, or in any other manner,
14 intentionally taps, or makes any unauthorized connection, whether physically, electrically,
15 acoustically, inductively, or otherwise, with any *telegraph or telephone* wire, line, cable, or
16 instrument, including the wire, line, cable, or instrument of any internal telephonic communication
17 system.” Cal. Penal Code § 631(a) (emphasis added). Defendant states that by referencing
18 “telegraph or telephone” lines, this first clause does not apply to communications over the internet.
19 *See* Dkt. No. 16 at 6–7. Plaintiff concedes that he received and accessed Defendant’s emails
20 “from his computer,” Compl. at ¶ 4, and that Bluecore tapped “the lines of internet
21 communication” between Plaintiff and Defendant, *id.* at ¶ 34. But Plaintiff disagrees that this
22 clause does not apply to the internet. *See* Dkt. No. 20 at 6–7.

23 Despite Plaintiff’s urging, however, courts have consistently interpreted this first clause as
24 applying only to tapping communications over telephones and not through the internet. *See, e.g.,*
25 *Cody v. Ring LLC*, No. 23-CV-00562-AMO, 2024 WL 735667, at *3 (N.D. Cal. Feb. 22, 2024)
26 (collecting cases); *Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751, 755–56 (N.D.
27 Cal. 2023); *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1079 (C.D. Cal. 2023);
28 *Williams v. What If Holdings, LLC*, No. C 22-03780 WHA, 2022 WL 17869275, at *2 (N.D. Cal.

Dec. 22, 2022). The Court finds the reasoning of these cases persuasive on this point and adopts it here.

The Court rejects Plaintiff’s argument to the contrary. Plaintiff points to a single district court case, *Kauffman v. Papa John’s Int’l, Inc.*, No. 22-CV-1492-L-MSB, 2024 WL 171363, at *8 (S.D. Cal. Jan. 12, 2024), that applied the first clause of § 631(a) to internet communications. *See* Dkt. No. 20 at 6–7. In *Kauffman*, the court acknowledged that the plain language of the first clause requires the plaintiff to “allege facts plausibly showing that [the defendant] or its vendor made an unauthorized connection with a ‘telegraph or telephone wire, line, cable, or instrument.’” *Id.* (quoting Cal. Penal Code § 631(a)). However, the court reasoned that the statute could—and should—be extended to new technologies, including the internet. *Id.* The Court respectfully disagrees with *Kauffman’s* brief analysis.

The California Supreme Court has recognized that courts are not precluded from applying statutes to technologies that did not yet exist at the time a statute was written. *See Apple Inc. v. Superior Ct.*, 56 Cal. 4th 128, 137 (Cal. 2013) (“Fidelity to legislative intent does not make it impossible to apply a legal text to technologies that did not exist when the text was created”) (quotation omitted). As the court explained, “[d]rafters of every era know that technological advances will proceed apace and that the rules they create will one day apply to all sorts of circumstances they could not possibly envision.” *Id.* (quotation omitted). But the court provided an important caveat: such an expansion is only appropriate if doing so does not conflict with the plain language and the statutory scheme. *See id.* at 137–39. Here, the first clause is not simply silent about what forms of technology and types of communications it applies to. Rather, it is specifically limited to “telegraph or telephone” communications, such that an expansion to other technologies would be inappropriate. *See* Cal. Penal Code § 631(a). The Court cannot ignore this language and rewrite the statute to apply more broadly.

The cases on which *Kauffman* relied also explicitly address the *second* clause of § 631(a), which unlike the first imposes liability for intercepting communications passing over “any wire, line, or cable.” Cal. Penal Code § 631(a) (emphasis added); *see also Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (interpreting the language in the

second clause when stating that “[t]hough written in terms of wiretapping, Section 631(a) applies to Internet communications”); *Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 8200619, at *18 (N.D. Cal. Aug. 12, 2016) (“[T]he second clause of section 631, as opposed to the first clause, is not limited to communications passing over ‘telegraph or telephone’ wires, lines, or cables.”); *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *20–21 (N.D. Cal. Sept. 26, 2013) (same). Because the language of the two clauses differs, the reasoning of these cases does not apply with equal force to expanding the scope of the first clause. The Court finds the first clause does not apply to internet communications, and **GRANTS** the motion to dismiss on this basis.

iii. Protected Content: Clauses Two through Four

Clauses two and three of § 631(a) prohibit the unauthorized access to and use of the “contents” of any communications, and clause four prohibits aiding and abetting such conduct. Cal. Penal Code § 631(a). Defendant urges that Plaintiff’s § 631(a) claim also fails because none of the information allegedly intercepted constitutes protected “contents” under the statute. *See* Dkt. No. 16 at 7–9. The definition of “contents” under CIPA is the same as under the Electronic Communications Privacy Act (“ECPA”). *See, e.g., In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022). The Ninth Circuit has held that under the ECPA “‘contents’ refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication.” *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)). In other words, courts must consider whether the intercepted information is “information *about* a user’s communication, or ‘the communication itself.’” *Id.* at 1107 (emphasis added). Only the latter is protected under CIPA.

Defendant argues that the complaint alleges that Bluecore’s software only captured record information about Defendant’s emails but not the “contents” of Defendant’s emails. *See* Dkt. No. 16 at 7–9. Specifically, the complaint alleges that when Plaintiff opened an email from Defendant, Bluecore intercepted “the time, date, device type, geolocation (and other information attributed to Mr. Ramos’s online activity) as well as his engagement with the Email’s content—including his

clicks on URL links embedded within the Emails’ Content.” *See* Compl. at ¶ 4. In opposition, Plaintiff appears to concede that such information would not constitute protected “contents” under the statute. *See* Dkt. No. 20 at 7 (arguing that Defendant has created a “strawman argument” by “cherry-pick[ing]” allegations about other information that Bluecore collects, such as “the time, place, device, geolocation, email address, and length of time spent”). However, Plaintiff suggests that there are other allegations in the complaint that Defendant ignores. *See id.*

Critically, however, Plaintiff does not identify this protected content with any level of specificity, and instead just gestures generally toward the complaint. For example, Plaintiff urges that “Defendant ignores Plaintiff’s allegations (including images) that show how Bluecore’s wiretaps capture the ‘contents’ of Defendant’s Emails.” *See* Dkt. No. 20 at 7 (citing Compl. at ¶¶ 10–14, 17–19). Although these paragraphs in the complaint explain how the Bluecore software allegedly works, they do not clearly identify the protected content of the communications at issue in this case. Elsewhere in his opposition, Plaintiff suggests that Bluecore receives “the entire contents of the Emails.” *See id.* at 3 (citing Compl. at ¶¶ 4, 10, 14, 17–19). But again, Plaintiff does not explain how this occurs. Later in his brief, Plaintiff contends that “Bluecore intercepted the URLs contained in the Emails without Plaintiff’s and Class Members’ consent.” *Id.* at 5 (citing Compl. at ¶¶ 1–2, 4, 10–14, 17–19, 35–36). Although perhaps more specific, Plaintiff still does not explain how the software intercepted any URLs. And in yet another part of his brief, Plaintiff states that “Defendant is directly liable under CIPA § 631(a) for monitoring the Email’s ‘open rates.’” *Id.* at 6. These conclusory assertions are not enough. Neither Defendant nor the Court should have to guess about such a fundamental piece of Plaintiff’s case.

As best as the Court can discern, Plaintiff appears to argue that the Bluecore software actually read the entire email from Defendant, including (1) undefined “email open rates” and (2) URLs linking to Defendant’s products on its website. *See id.* at 3, 5–9. Neither theory is sufficiently alleged, and in his opposition, Plaintiff mischaracterizes the allegations in the complaint in an effort to support these theories. This post hoc shapeshifting is clearly improper.

First, “email open rates” in this context are not content. Although Plaintiff does not define the term, as discussed in Section III.A.i above, the only plausible interpretation is that this refers to

a datapoint about how many of Defendant’s emails a consumer has opened. Such a data point is thus equivalent to a “read receipt,” indicating that a consumer received and opened a message. As such, it falls squarely within the definition of “record information” because it is not about the content of the emails at all.

Second, the complaint does not allege that the Bluecore software actually read the contents of Defendant’s emails at all. Plaintiff’s suggestion otherwise is simply wrong and raises serious credibility issues. The complaint alleges in relevant part:

- “Plaintiff received and interacted with Defendant’s Emails on multiples occasions” Compl. at ¶ 4.
- When Plaintiff opened an email, the software intercepted “the time, date, device type, geolocation (and other information attributed to Mr. Ramos’s online activity) as well as his engagement with the Email’s content—including his clicks on URL links embedded within the Emails’ Content.” *Id.*
- The software “embeds an invisible URL link within the clickable images and words included in the body of the email.” *See id.* at ¶ 11. Plaintiff elsewhere refers to the email’s “clickable images and words” as the email’s content. *Id.* at ¶ 14. When a customer “clicks on a trackable URL link, the customers are directed to Bluecore’s servers, permitting Bluecore to capture a large amount of data, such as the recipient’s email address as well as email open rates and content click rates.” *Id.* at ¶ 11; *see also id.* at ¶ 14.
- “Through its Email and Website wiretaps, Bluecore intercepts, at a minimum . . . Emails,” specifically “the time, place, device geolocation, email address, and open rates and click rates of Emails (including what part of the Email’s Content was clicked on).” *Id.* at ¶ 19.

The complaint therefore refers to capturing information *about* the emails, such as “email open rates” and “click rates.” But Plaintiff does not explain how such information constitutes protected content under the statute. The complaint says nothing about reading or otherwise capturing “the

clickable images and words included in the body of the email,” which the complaint refers to as the actual email content. *See id.* at ¶ 14.

In his opposition brief, Plaintiff attempts to argue that URLs are content. *See* Dkt. No. 20 at 8 (citing *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 265 (N.D. Cal. 2016)). While that may be true in some circumstances, the complaint does not plausibly allege so here. To the extent the complaint references URLs at all, it does not allege that the software reads these URLs.

According to the complaint, the software creates its own “invisible URL link.” Compl. at ¶ 11.

This link appears to belong to Bluecore. *See id.* (“Bluecore embeds an invisible URL link within the clickable images and words included in the body of an email.”). And rather than convey any intended message, Plaintiff’s allegations indicate that these URLs are “hidden” and serve a tracking or routing function. *See, e.g., id.* at ¶ 11 (“When the recipient of an email clicks on a trackable URL link, the customers are directed to Bluecore’s servers, permitting Bluecore to capture a large amount of data, such as the recipient’s email address as well as email open rates, and content click rates.”); *id.* at ¶ 14 (“When a user clicks on the content of the email to be directed to a particular webpage within a website (*e.g.*, a specific shirt showcased in the email), Bluecore immediately intercepts the communication and gathers valuable data (including the email address of the subscriber as well as his or her device type, geolocation, IP address and the part of the email he or she clicked on).”). Nothing in the complaint suggests that these URLs are related to the “substance, purport, or meaning” of Defendant’s emails. *Zynga*, 750 F.3d at 1104.

In support of his argument, Plaintiff points to a single allegation in the complaint, which concludes that “the Bluecore tracking software *read with specificity the Emails sent by Defendant* which Plaintiff and the Class members read and replied to by clicking on the URL link embedded within the content of the Emails.” *See* Dkt. No. 20 at 7 (citing Compl. at ¶ 36) (emphasis added). In other words, Plaintiff suggests that the tracking software can read the *content* of the emails that Defendant sends to its customers. But this allegation is in tension with the earlier allegations in the complaint in which Plaintiff describes only discrete parts of the emails that Bluecore intercepts, such as “what part of the Email’s Content was clicked on.” *See* Dkt. No. 23 at 8 (citing Compl. at ¶ 19). Even when read in the light most favorable to Plaintiff, as the Court must do at

1 this stage, the complaint simply offers no support for the conclusory statement that the software
2 “reads with specificity” Defendant’s emails.

3 Additionally, Plaintiff asks the Court to consider the information that the Bluecore
4 software collects on Defendant’s website. *See* Dkt. No. 20 at 8. For example, Plaintiff states that
5 the software collects information such as “email capture . . . when an email address is entered [into
6 a ‘popup’].” *See id.* (citing Compl. at ¶¶ 14, 19). Even assuming this constitutes protected
7 content, however, Plaintiff does not allege that he ever entered any information into a popup on
8 Defendant’s website. Plaintiff offers no detail about his use of Defendant’s website. He only
9 broadly states that he was directed to web pages on Defendant’s website, and was unaware that
10 “his engagement with . . . the Website” was being intercepted. *See* Compl. at ¶ 4. Plaintiff has
11 failed to allege that the Bluecore software intercepted any protected content for purposes of CIPA,
12 and the Court therefore **GRANTS** the motion to dismiss on this basis.

13 **B. Remaining Causes of Action**

14 Defendant urges that because Plaintiff’s claim under § 631(a) fails, his claim under CIPA
15 § 635, statutory larceny, and the UCL necessarily fail too. *See* Dkt. No. 16 at 9–15. Plaintiff
16 appears to agree that these claims rise and fall together because they are based on wiretapping
17 protected “content.” *See* Dkt. No. 20 at 9–12, 16–18. Because the Court agrees with Defendant
18 that Plaintiff has failed to plead the interception of such protected content, the Court **GRANTS** the
19 motion to dismiss Plaintiff’s remaining causes of action as well.

20 **C. UCL**

21 Lastly, Defendant raises several procedural problems with Plaintiff’s UCL claim. He
22 argues that Plaintiff cannot seek injunctive relief under the UCL because he has failed to allege
23 that he lacks an adequate remedy at law. *See* Dkt. No. 16 at 12–13. Defendant also urges that
24 Plaintiff failed to allege that he lost money or property sufficient to satisfy the UCL’s statutory
25 standing requirements. *See id.* at 13–15. To enable Plaintiff to effectively amend the complaint,
26 the Court briefly addresses these two arguments.

27 **i. Equitable Relief**

28 “In order to entertain a request for equitable relief, a district court must have equitable

jurisdiction, which can only exist under federal common law if the plaintiff has no adequate legal remedy.” *Guzman v. Polaris Indus.*, 49 F.4th 1308, 1313 (9th Cir. 2022). Although this Court has, in the past, noted *Sonner’s* odd procedural posture, the Ninth Circuit in *Guzman* has indicated that *Sonner’s* holding was not limited to its posture. *See id.* Here, Plaintiff urges that he is pleading in the alternative. *See* Dkt. No. 20 at 12. But even so, he admits that he does not allege that he lacks an adequate remedy at law. *See id.* Plaintiff states that such an argument is “highly formalistic” and “easily fixable.” *See id.* at 12–13. But Plaintiff’s own authorities indicate that this is nevertheless a pleading requirement. *See Mikulsky v. Bloomingdale’s, LLC*, No. 3:23-CV-00425-L-VET, 2024 WL 337180, at *8 (S.D. Cal. Jan. 25, 2024). Because Plaintiff has failed to plead that a remedy at law is inadequate, he cannot seek equitable relief. *Id.*

ii. Statutory Standing

In addition to the requirements of Article III standing, the UCL has additional standing requirements that require plaintiffs to (1) plead an economic injury and (2) show that the injury was caused by the challenged conduct. *See Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322 (Cal. 2011). Plaintiff responds that he adequately alleged that he lost money as a result of Defendant’s conduct because he “has suffered harm in the form of diminution of the value of his private and personally identifiable data and online activities.” *See* Dkt. No. 20 at 14 (citing Compl. ¶ 69). But as already discussed, Plaintiff has not sufficiently alleged exactly what data was intercepted here. Plaintiff contends that it was “private and personally identifiable data and online activities,” *id.*, and that this data was “extensive,” *id.* at 15. But such conclusory allegations are obviously insufficient.

IV. CONCLUSION


The Court **GRANTS** the motion to dismiss. Dkt. No. 16. At this stage in the litigation, the Court cannot say that amendment would be futile. Plaintiff may therefore file an amended complaint within 21 days of the date of this order provided counsel can do so consistent with their Rule 11 obligations. Plaintiff’s counsel is further warned that they need to fully plead their best case in any amended complaint: it is an inefficient use of everyone’s resources to dribble out the key allegations over the course of multiple complaints, and there is no guarantee that the Court

1 will grant further leave to amend.

2 The Court further **SETS** case a case management conference on November 19, 2024, at
3 2:00 p.m. The hearing will be held by Public Zoom Webinar. All counsel, members of the public,
4 and media may access the webinar information at <https://www.cand.uscourts.gov/hsg>. The parties
5 are further **DIRECTED** to file a joint case management statement by November 12, 2024.

6 **IT IS SO ORDERED.**

7 Dated: 9/30/2024

8 
9 HAYWOOD S. GILLIAM, JR.
United States District Judge